WOJEWODA
WARMIŃSKO-MAZURSKI
Artur Chojecki

FK-IV.431.5.2020

Olsztyn, 2 kwietnia 2020 r.

Szanowny Pan
Sławomir Ambroziak
Wójt Gminy Jedwabno
ul. Warmińska 2
12-122, Jedwabno

Stosownie do art. 47 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224), , przekazuję Panu treść wystąpienia pokontrolnego.

Wystąpienie pokontrolne

Kontrolę przeprowadzono w Urzędzie Gminy w Jedwabnie, ul. Warmińska 2, 12-122 Jedwabno, NIP: 7450005403, REGON: 000535623.

W okresie objętym kontrolą stanowisko kierownika jednostki kontrolowanej pełnił Pan **Sławomir Ambroziak** – Wójt Gminy Jedwabno, wybrany na stanowisko w wyniku wyborów bezpośrednich w dniu 20 listopada 2018 roku.

Odpowiedzialnymi za realizację zadania w Urzędzie Gminy byli:
1. Informatyk Urzędu – zatrudniony na samodzielnym stanowisku pracy. Zgodnie z informacją uzyskaną z jednostki, zrezygnował z pracy w Urzędzie z dniem 9 lutego 2020r.
2. Inspektor Ochrony Danych, świadczący usługę IOD na rzecz Urzędu Gminy Jedwabno zgodnie z podpisana umową.

[akta kontroli str. 60-66, 68-74]

Kontrolę przeprowadził pracownik Wydziału Finansów i Kontroli Warmińsko- Mazurskiego Urzędu Wojewódzkiego w Olsztynie, Radosław Gazda – inspektor wojewódzki; legitymacja służbowa nr 9/2019, wydana przez Dyrektora Generalnego Warmińsko - Mazurskiego Urzędu Wojewódzkiego w Olsztynie – na podstawie pisemnego imiennego upoważnienia do kontroli nr FK-IV.0030.106.2020 z 5 lutego 2020 r., wydanego przez Wojewodę Warmińsko-Mazurskiego.

[akta kontroli str. 57]

Kontrolę przeprowadzono w dniach 26-27 lutego oraz w dniu 2 marca 2020 r., co zostało odnotowane w książce kontroli Urzędu Gminy pod pozycją Nr 2/2020.

Przedmiotem kontroli była ocena działania systemów teleinformatycznych używanych przez jednostki samorządu terytorialnego do realizacji zadań zleconych z zakresu administracji rządowej, na podstawie art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570 ze zm. - akt prawny obowiązujący do 02.04.2019 r. oraz Dz.U. z 2019 r. poz. 700 ze zm.). Okres objęty kontrolą: od dnia 1 stycznia 2018 r. do dnia 26 lutego 2020 r. (dzień rozpoczęcia czynności kontrolnych).

[akta kontroli str. 1, 36, 57]

Kontrola została przeprowadzona na podstawie art. 2 pkt 1 i art. 6 ust. 4 pkt 3 ustawy z dnia 15 lipca 2011 r. o kontroli w administracji rządowej (Dz.U. 2020 poz. 224) oraz art. 28 ust. 1 pkt 2 ustawy z dnia 23 stycznia 2009 r. o wojewodzie i administracji rządowej w województwie (Dz. U. z 2019 r., poz. 1464) w związku z art. 25 ust. 1 pkt 3 lit. a ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2017 r. poz. 570 ze zm. - akt prawny obowiązujący do 02.04.2019 r. oraz Dz.U. z 2019 r. poz. 700 ze zm.), zwanej dalej „ustawą" oraz rozdziału III i IV Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. z 2017 r. poz. 2247 ze zm.), zwanego dalej „rozporządzeniem KRI", jak również Wytycznych dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych, zatwierdzonych przez Ministra Cyfryzacji w dniu 15 grudnia 2015 r.

[akta kontroli str. 1, 36, 57]

W czasie trwania czynności kontrolnych informacji i wyjaśnień udzielali:
- Sekretarz Gminy Jedwabno,
- Inspektor Ochrony Danych, świadczący usługę IOD na rzecz Urzędu Gminy Jedwabno.

[akta kontroli str. 67-74]

Na podstawie ustaleń kontroli, realizację zadań z zakresu działania systemów teleinformatycznych używanych przez Urząd do realizacji zadań zleconych z zakresu administracji rządowej ocenia się **pozytywnie z nieprawidłowościami.**
Ocena działalności jednostki kontrolowanej wynika z ustaleń i ocen dokonanych w poszczególnych obszarach (zagadnieniach) objętych kontrolą.

Z informacji przekazanych przez UG Jedwabno przed rozpoczęciem czynności kontrolnych oraz uzyskanych w trakcie prowadzenia kontroli wynika, że w Urzędzie do realizacji zadań

zleconych z zakresu administracji rządowej wykorzystywane są **3** systemy teleinformatyczne (Źródło – 2 moduły, PUMA – 2 moduły, CEIDG).

Systemy teleinformatyczne wykorzystywane w Urzędzie Gminy Jedwabno:

1) **ŹRÓDŁO** – **(Rejestr PESEL, Rejestr dowodów osobistych)** bezpłatna aplikacja, która obsługuje wszystkie wymagane polskim prawem działania w zakresie rejestru PESEL, dowodów osobistych. Dodatkowo umożliwia również realizację zadań Systemu Odznaczeń Państwowych oraz Centralnego Rejestru Sprzeciwów. W efekcie ŹRÓDŁO to uniwersalne narzędzie obsługujące m.in.: Rejestr PESEL, Rejestr Bazy Usług Stanu Cywilnego (BUSC), Rejestr Dowodów Osobistych (RDO), System Odznaczeń Państwowych (SOP), Centralny Rejestr Sprzeciwów (CRS).

2) **PUMA - Moduł Ewidencja Ludności (rejestr mieszkańców)** posiada homologację MSW, a jego zadaniem jest kompleksowa obsługa komórki ewidencji ludności. Aplikacja umożliwia między innymi: gromadzenie, wyszukiwanie, uzupełnianie oraz zmianę w bazie danych wszystkich informacji znajdujących się na Karcie Osobowej Mieszkańca. Program automatyzuje pracę i drukuje zawiadomienia w zakresie: meldowania, wymeldowania, rejestracji urodzeń, zgonów, zmian stanu cywilnego, gromadzenia i dostępu do danych historycznych mieszkańców.
Moduł Wyborcy - kompleksowa obsługa wyborów. Moduł Wyborcy umożliwia prowadzenie i aktualizację rejestru wyborców, sporządzanie spisów wyborców uprawnionych do udziału w wyborach i referendum, pozwala na generowanie kwartalnych meldunków dla KBW (Krajowego Biura Wyborczego) o stanie wyborców mieście na podstawie bazy danych ewidencyjnych.

3) **CEIDG** jest to elektroniczny rejestr przedsiębiorców działających na terenie kraju. Portal ułatwia podatnikom prowadzenie działalności gospodarczej. Umożliwia on założenie firmy, aktualizację danych, jak również zamknięcie czy zawieszenie działalności gospodarczej. Służy również do przekazywania informacji o wydanych zezwoleniach, koncesjach oraz wpisach do rejestrów.

Rejestry publiczne i ewidencje prowadzone w Urzędzie Gminy w Jedwabnie:

- Rejestr działalności regulowanej w zakresie odbierania odpadów komunalnych od właścicieli nieruchomości (podstawa prawna - art. 9b ust. 2-3 ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, t. j. Dz. U. z 2019 r., poz. 2010 ze zm.).
- Ewidencja podmiotów zajmujących się opróżnianiem zbiorników bezodpływowych i transportem nieczystości ciekłych na terenie Gminy Jedwabno.
- Rejestr instytucji kultury dla których organizatorem jest Gmina (podstawa prawna art. 14 ust. 1 ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności

kulturalnej).

[akta kontroli str. 75-80]

I. Wymiana informacji w postaci elektronicznej, w tym współpraca z innymi systemami/rejestrami informatycznymi i wspomaganie świadczenia usług drogą elektroniczną.

1.1. Usługi elektroniczne

Z art. 16 ust. 1a ustawy wynika, że *podmiot publiczny udostępnia elektroniczną skrzynkę podawczą, spełniającą standardy określone i opublikowane na ePUAP przez ministra właściwego do spraw informatyzacji, oraz zapewnia jej obsługę.*

Zgodnie z § 5 ust. 2 pkt 1 i 4 rozporządzenia KRI interoperacyjność na poziomie organizacyjnym osiągana jest przez:

a) informowanie przez podmioty realizujące zadania publiczne, w sposób umożliwiający skuteczne zapoznanie się, o sposobie dostępu oraz zakresie użytkowym serwisów dla usług realizowanych przez te podmioty;

b) publikowanie i uaktualnianie w Biuletynie Informacji Publicznej przez podmiot realizujący zadania publiczne opisów procedur obowiązujących przy załatwianiu spraw z zakresu jego właściwości drogą elektroniczną.

Urząd Gminy Jedwabno posiada aktywną Elektroniczną Skrzynkę Podawczą **/5b30r2fhow/skrytka** znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiającą doręczanie i odbieranie pism w formie dokumentów elektronicznych. Szczegółowe informacje dotyczące funkcjonowania oraz możliwość bezpośredniego przejścia na główną stronę e-PUAP, zawarto na stronie internetowej BIP Urzędu, Menu przedmiotowe - Urząd Gminy - Elektroniczna skrzynka podawcza.
Formaty danych przyjmowane za pośrednictwem Elektronicznej Skrzynki Podawczej to m.in.: ODF, ODS, DOC, RTF, XLS, CSV, TXT, PNG, GIF, TIF, BMP, JPG, PDF, ZIP, RAR, 7zip.

W zakresie publikacji procedur załatwiania spraw realizowanych przez Urząd należy stwierdzić, iż na stronie BIP w zakładce Menu przedmiotowe – Formularze do pobrania, opublikowane są wzory wniosków i formularzy, będących w zakresie poszczególnych referatów w Urzędzie.
Urząd Gminy w Jedwabnie wdrożył również projekt centralnej platformy e-usług dla mieszkańca. Za pomocą powyższej aplikacji publikowane są wzory wniosków, deklaracje, formularze (zakładka eBOI - Karty usług) dostępne dla każdego mieszkańca, w zakresie poszczególnych usług oferowanych przez Urząd w ramach centralnej platformy e-usług.
Urząd nie świadczył usług związanych z załatwianiem spraw od początku do końca w formie elektronicznej, za pomocą systemów teleinformatycznych.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 306, 314-317]

1.2. Centralne repozytorium wzorów dokumentów elektronicznych (CRWDE)

Stosownie do art. 19b ust. 3 ustawy, *organy administracji publicznej przekazują do centralnego repozytorium oraz udostępniają w Biuletynie Informacji Publicznej wzory dokumentów elektronicznych. Przy sporządzaniu wzorów dokumentów elektronicznych stosuje się międzynarodowe standardy dotyczące sporządzania dokumentów elektronicznych przez organy administracji publicznej, z uwzględnieniem konieczności podpisywania ich kwalifikowanym podpisem elektronicznym.*

W celu ujednolicenia w skali kraju procedur usług świadczonych przez urzędy drogą elektroniczną, w tym ujednolicenia wzorów dokumentów elektronicznych w CRWDE przechowywane są wzory dokumentów, jakie zostały już opracowane i są używane. W przypadku uruchamiania przez dany podmiot publiczny usługi elektronicznej, która funkcjonuje już na koncie innego podmiotu, dany podmiot publiczny powinien skorzystać z procedury obsługi tej usługi oraz zastosować wzory dokumentów elektronicznych dotyczące tej procedury znajdujące się w CRWDE (nie dotyczy to sytuacji gdy usługa jest usługą centralną, tzn. jest udostępniania przez jeden podmiot, np. właściwego ministra, ale służy do świadczenia usług przez inne podmioty niż udostępniający, np. wszystkie gminy). W przypadku uruchamiania usługi, dla której nie ma wzorów dokumentów w CRWDE, podmiot publiczny jest zobowiązany przekazać do CRWDE procedurę obsługi usługi i wzory dokumentów elektronicznych z nią związanych.

W trakcie kontroli ustalono, że Urząd Gminy w badanym okresie nie przekazywał wzorów dokumentów elektronicznych do centralnego repozytorium wzorów dokumentów prowadzonego przez Ministerstwo Cyfryzacji, ze względu na fakt, iż nie uruchamiał nowej usługi, dla której nie ma wzorów dokumentów w CRWDE.
Z wyjaśnienia uzyskanego w powyższej sprawie z Urzędu Gminy wynika, że cyt.: *„Urząd Gminy przekazywał do ePUAP wzory dokumentów elektronicznych i korzystał z dokumentów zamieszczonych w CRWDE. (w załączeniu wydruk strony https://e.jedwabno.pi zakładka e-usługi - system eBOI)".*
Jednocześnie należy zaznaczyć, iż na stronie BIP kontrolowanego Urzędu opublikowano w wersji „do pobrania" formularze niektórych wzorów dokumentów niezbędnych do załatwienia poszczególnych spraw w Urzędzie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 306, 308, 316, 442-, 445-447]

1.3. Model usługowy

- Z § 15 ust. 2 rozporządzenia KRI wynika, że *zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.*

Strona internetowa Urzędu działa pod adresem https://www.jedwabno.pl/, a strona internetowa BIP Urzędu – pod adresem https://bip.jedwabno.pl/.
Na stronie internetowej Urzędu zamieszczono bezpośredni link do strony BIP Urzędu w górnej części panelu strony. Na stronie głównej BIP Urzędu zamieszczono link do skrzynki podawczej ESP na platformie ePUAP.
Ponadto na stronie internetowej BIP UG https://bip.jedwabno.pl/, znajdują się linki do najważniejszych serwisów internetowych ułatwiających odbiorcy internetowemu załatwienie podstawowych spraw urzędowych, tj.:

- **OBYWATEL.GOV.PL**, który powstał jako część programu pl.ID, realizowanego w ramach Programu Operacyjnego Innowacyjna Gospodarka (7. Oś priorytetowa – Społeczeństwo informacyjne – budowa elektronicznej administracji) i współfinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego. Znajduje się tu kilkaset najpopularniejszych usług świadczonych przez administrację publiczną.
- **CEiDG** - Centralna Ewidencja i Informacja o Działalności Gospodarczej (CEIDG) – jest to rejestr przedsiębiorców, którzy są osobami fizycznymi, działającymi na terenie Polski. Rejestr prowadzony jest w formie systemu teleinformatycznego przez ministra właściwego do spraw gospodarki. Rejestracja w CEIDG jest bezpłatna. Wpisowi do ewidencji podlegają przedsiębiorcy będący osobami fizycznymi. Przedsiębiorca może podjąć działalność gospodarczą w dniu złożenia wniosku o wpis do CEIDG albo po uzyskaniu wpisu do rejestru przedsiębiorców w Krajowym Rejestrze Sądowym (KRS). Wpis dokonywany jest nie później, niż następnego dnia roboczego po dniu wpływu do CEIDG poprawnego wniosku. Zaświadczeniem o wpisie do CEIDG jest wydruk ze strony internetowej CEIDG.
- **EMP@TIA** - portal informacyjno-usługowy Ministerstwa Rodziny Pracy i Polityki Społecznej, za pomocą którego istnieje możliwość złożenia wniosku elektronicznego.
- **ePUPAP** - elektroniczna skrzynka podawcza znajdującą się na Elektronicznej Platformie Usług Administracji Publicznej, umożliwiająca doręczanie pism w formie dokumentów elektronicznych.

Urząd Gminy w Jedwabnie wdrożył projekt centralnej platformy e-usług dla mieszkańca. Każdy zarejestrowany na platformie mieszkaniec gminy może skorzystać z portalu e-usługi, umożliwiającego:

- prezentację stanów indywidualnych kont kontrahentów,
- otrzymywanie powiadomień o zbliżających się terminach płatności należności,
- otrzymywanie powiadomień o ważnych wydarzeniach dla mieszkańców gminy,
- korzystanie z formularzy elektronicznych przygotowanych dla mieszkańców i kontrahentów.

W związku z wdrożeniem projektu centralnej platformy e-usług dla mieszkańca,

zarządzeniem Nr 102/2019 Wójta Gminy Jedwabno z dnia 23 października 2019 r., w sprawie wprowadzenia usług świadczonych drogą elektroniczną oraz wprowadzeniu Regulaminu użytkownika usług świadczonych drogą elektroniczną, określono katalog usług które mogą być świadczone w Urzędzie za pośrednictwem platformy ePUAP w formie elektronicznej.

W Urzędzie brak jest formalnych procedur opisujących obsługę oraz monitorowanie usług elektronicznych za pomocą systemów teleinformatycznych, ze względu na fakt, iż instytucja ta nie świadczyła usług elektronicznych na zewnątrz za pomocą systemów teleinformatycznych wykorzystywanych do realizacji zadań zleconych z zakresu administracji rządowej, w związku z powyższym przedmiotowe cząstkowe zagadnienie nie podlegało ocenie.

[akta kontroli str. 298-313]

1.4. Współpraca systemów teleinformatycznych z innymi systemami

Stosownie do:

- § 5 ust. 3 pkt 3 rozporządzenia KRI *interoperacyjność na poziomie semantycznym osiągana jest przez: stosowanie w rejestrach prowadzonych przez podmioty publiczne odwołań do rejestrów zawierających dane referencyjne w zakresie niezbędnym do realizacji zadań;*
- § 16 ust. 1 rozporządzenia KRI *systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.*

Wiele rejestrów w urzędach administracji publicznej przechowuje i przetwarza identyczne informacje, np. o obywatelu/podmiocie, takie jak PESEL, REGON, NIP, dane adresowe itp. Ułatwieniem w załatwieniu spraw dla obywatela lub podmiotu będzie sytuacja, gdy podmiot publiczny nie będzie żądał od obywatela lub podmiotu informacji będących już w posiadaniu urzędów. Realizacja tego postulatu wymaga, aby system informatyczny, w którym prowadzony jest dany rejestr odwoływał się bezpośrednio do danych gromadzonych w innych rejestrach publicznych uznanych za referencyjne w zakresie niezbędnym do realizacji zadań.

Z informacji uzyskanych z Urzędu (ankieta zał. nr 1) wynika, że, cyt.: *„System informatyczny używany w Urzędzie – PUMA współpracuje z systemem publicznym ŹRÓDŁO. Komunikacja jest możliwa dzięki wyposażeniu w składniki sprzętowe i oprogramowanie umożliwiające wymianę danych między tymi systemami."*

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 19]

1.5. Obieg dokumentów w podmiocie publicznym

Z § 20 ust. 2 pkt 9 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie.*

Zgodnie z zarządzeniem Nr 11/2011 Wójta Gminy Jedwabno z dnia 02.03.2011 r. w sprawie systemu czynności kancelaryjnych w Urzędzie Gminy w Jedwabnie, wskazano system tradycyjny (papierowy) jako system podstawowy wykonywania czynności kancelaryjnych (zarządzenie obowiązywało do dnia 1 października 2019 r.).
Zgodnie z zarządzeniem Nr 95/2019 Wójta Gminy Jedwabno z dnia 30 września 2019 r. w sprawie wprowadzenia Systemu Elektronicznego Obiegu Dokumentów przy wykorzystaniu systemy EDICTA w Urzędzie Gminy Jedwabno, podstawowym sposobem dokumentowania przebiegu załatwiania spraw w Urzędzie jest system tradycyjny. Elektroniczny system obiegu dokumentów jest systemem wspomagającym. EDICTA to elektroniczny system obsługi dokumentów określający sposób doręczania i wysyłania korespondencji w postaci elektronicznej. Umożliwia zarządzanie dokumentami, korespondencją, sprawami (projektami), poleceniami, terminami oraz czasem pracy pracowników, tworząc centralną, uporządkowaną bazę dokumentów i informacji. Umożliwia również sprawny dostęp do korespondencji, umów, procedur wewnętrznych itp., kontroluje drogę obiegu korespondencji oraz stan realizacji projektów, usprawnia obsługę klientów.
W zarządzeniu określono sposób postępowania z korespondencją wpływającą i wypływającą z Urzędu w formie elektronicznej, co zgodnie z § 20 ust. 2 pkt 9 rozporządzenia KRI, umożliwia realizację i egzekwowanie, m.in. zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie.

W związku z powyższym przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 81-92]

1.6. Formaty danych udostępniane przez systemy teleinformatyczne

Stosownie do:

- § 17 ust. 1 rozporządzenia KRI *kodowanie znaków w dokumentach wysyłanych z systemów teleinformatycznych podmiotów realizujących zadania publiczne lub odbieranych przez takie systemy, także w odniesieniu do informacji wymienianej przez te systemy z innymi systemami na drodze teletransmisji, o ile wymiana ta ma charakter wymiany znaków, odbywa się według standardu Unicode UTF-8 określonego przez normę ISO/IEC 10646 wraz ze zmianami lub normę ją zastępującą;*

- § 18 ust. 1 rozporządzenia KRI *systemy teleinformatyczne podmiotów realizujących zadania publiczne udostępniają zasoby informacyjne co najmniej w jednym z formatów danych określonych w załączniku nr 2 do rozporządzenia;*
- § 18 ust. 2 rozporządzenia *KRI jeżeli z przepisów szczegółowych albo opublikowanych w repozytorium interoperacyjności schematów XML lub innych wzorów nie wynika inaczej, podmioty realizujące zadania publiczne umożliwiają przyjmowanie dokumentów elektronicznych służących do załatwiania spraw należących do zakresu ich działania w formatach danych określonych w załącznikach nr 2 i 3 do rozporządzenia.*

Istotą współdzielenia informacji w urzędach jest stworzenie możliwości wymiany danych pomiędzy różnymi systemami informatycznymi oraz umożliwienie odbiorcom swobodnego dostępu do informacji poprzez wygenerowanie danych w powszechnie znanych i dostępnych formatach plików.

Z informacji uzyskanych z Urzędu (ankieta zał. nr 1) wynika, że, cyt.: *„System PUMA pobiera dane bezpośrednio z systemu ŹRÓDŁO za pomocą aplikacji dostarczonej przez Zeto Software (producenta oprogramowania). Dane przekazywane są w formacie XML (kodowane w standardzie Unicode UTF-8). Moduł Ewidencja Ludności posiada homologację MSW".*

[akta kontroli str. 20]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

II. System zarządzania bezpieczeństwem informacji w systemach teleinformatycznych

2.1. Dokumenty z zakresu bezpieczeństwa informacji

Zgodnie z:

- § 20 ust. 1 rozporządzenia KRI *podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność;*
- § 20 ust. 2 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie działań związanych z bezpieczeństwem informacji;*
- § 20 ust. 2 pkt 1 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia.*

Podmiot publiczny realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania

bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji. Wymaga to opracowania dokumentacji SZBI (system zarządzania bezpieczeństwem informacji), w tym szeregu regulacji wewnętrznych oraz zapewnienia aktualizacji tych regulacji w zakresie dotyczącym zmieniającego się otoczenia. Kompleksowa dokumentacja SZBI jest warunkiem niezbędnym, w celu skutecznego zarządzania bezpieczeństwem informacji w podmiocie.
Podstawowym dokumentem SZBI jest Polityka Bezpieczeństwa Informacji. Polityka zazwyczaj zawiera wyrażoną przez kierownictwo deklarację stosowania, opisuje organizację i ustala osoby odpowiedzialne oraz ich zakresy odpowiedzialności, wprowadza klasyfikację informacji, sposób postępowania z poszczególnymi rodzajami informacji.

- Zarządzeniem 60/2015 Wójta Gminy Jedwabno z dnia 30 czerwca 2015 r. r. wdrożono Politykę Bezpieczeństwa Przetwarzania Danych Osobowych w Urzędzie Gminy Jedwabno.
- Zarządzeniem 61/2015 Wójta Gminy Jedwabno z dnia 30 czerwca 2015 r. r. wdrożono Instrukcję Zarządzania Systemem Informatycznym Służącym do Przetwarzania Danych Osobowych w Urzędzie Gminy Jedwabno.

Obydwa zarządzenia wprowadzono zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (Dz.U. 2014 r., Nr 101, poz. 1182 ze zm.) oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. z 2004 r. Nr 100, poz. 1024).
Powyższa dokumentacja, (Polityka bezpieczeństwa przetwarzania danych osobowych oraz Instrukcja zarządzania systemem informatycznym), stanowiła dokumentację przetwarzania danych osobowych w rozumieniu §1 pkt 1 rozporządzenia MSWiA z 29 kwietnia 2004 r., w sprawie dokumentacji przetwarzania danych osobowych (...). Służyła ona zapewnieniu poufności, integralności i rozliczalności przetwarzanych danych.

[akta kontroli str. 93-140]

- W związku z wejściem w życie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27.04.2016 roku, w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119, s.1) – zwanego dalej „RODO", Zarządzeniem Nr 80/2018 Wójta Gminy Jedwabno z dnia 27 lipca 2018 r. wprowadzono Politykę Bezpieczeństwa w Urzędzie Gminy Jedwabno (zmiana - zarządzenie Nr 116/2018 Wójta Gminy Jedwabno z dnia 15 listopada 2018 r.). Dokumentację sporządzono na podstawie obowiązujących przepisów prawa, tj. „RODO" oraz ustawy dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000), w brzmieniu obowiązującym w tym okresie. Dokumentacja w zakresie ochrony danych dotyczyła danych przetwarzanych w Urzędzie i służyła zapewnieniu poufności, integralności przetwarzania danych, jak również monitorowania

zdarzeń naruszających ochronę danych (w tym osobowych), zawierała także opis postępowania w przypadku naruszenia zasad bezpieczeństwa danych osobowych.

[akta kontroli str. 141-297]

- Wójt Gminy Jedwabno wyznaczył Administratora Systemu Informatycznego (Informatyk Urzędu).
- Wójt Gminy Jedwabno podpisał stosowne umowy z firmą zewnętrzną na świadczenie usług Inspektora Ochrony Danych w Urzędzie, zgodnie z art. 39 RODO.

[akta kontroli str. 62-66, 68-74]

Inspektor Ochrony Danych, przeprowadził w 2018 roku 7 sprawdzeń/przeglądów przestrzegania przyjętych procedur ochrony danych osobowych w Urzędzie. W wyniku prowadzonych czynności sprawdzających nie wykryto istotnych nieprawidłowości.
W 2019 roku Inspektor Ochrony Danych, zgodnie z przyjętym harmonogramem sprawdzeń zaplanował w kolejnych kwartałach roku przeprowadzenie sprawdzenia w zakresie:

- I kw. 2019 r. – „Weryfikacja procedury aktualizacji oprogramowania". Przedmiotowa weryfikacja została przeprowadzona. Stwierdzono brak informacji o wykonywaniu kopii zapasowych w zakresie systemu PUMA, brak monitorowania oprogramowania antywirusowego, brak informacji o przekazaniu haseł do ADO, brak informacji o jakimkolwiek testowym odtworzeniu kopii systemu PUMA. Wnioski z przeprowadzonych sprawdzeń przekazane zostały Wójtowi Gminy.
- II kw. 2019 r. – „Weryfikacja procedur przechowywania haseł i dokumentacji konfiguracyjnej". Zaplanowane sprawdzenie nie zostało przeprowadzone. Zgodnie z informacją przekazaną Wójtowi Gminy, ASI (informatyk) nie udostępnił IOD stosownych dokumentów.
- III kw. 2019 r. – „Zachowanie zasad czystego biurka". Zaplanowane sprawdzenia zostały przeprowadzone na 15 stanowiskach roboczych. Wszystkie spełniały przyjęte zasady.
- IV kw. 2019 r. – „Przechowywanie dokumentacji elektronicznej na dyskach". Zaplanowane sprawdzenie nie zostało przeprowadzone. Zgodnie z informacją przekazaną Wójtowi Gminy, ASI (informatyk) nie udostępnił IOD stosownych dokumentów.

Brak realizacji przyjętego harmonogramu poprzez niewykonanie zaplanowanych sprawdzeń w II i IV kw. 2019 r. stanowi nieprawidłowość skutkującą naruszeniem § 20 ust. 1 rozporządzenia KRI, który stanowi, że *podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji.* Osobami odpowiedzialnymi za powstanie nieprawidłowości są pracownik odpowiedzialny za realizację zadania (Informatyk Urzędu) oraz osoba bezpośrednio go nadzorująca.

W 2020 roku zgodnie z przyjętym harmonogramem sprawdzeń na każdy kwartał roku zaplanowano wykonanie jednego zadania sprawdzającego. Przeprowadzenie zaplanowanego w I kw. sprawdzenia nie zostało poddane ocenie ze względu na istniejącą możliwość jego przeprowadzenia do końca kwartału.

[akta kontroli str. 348-371]

W 2019 roku przeprowadzone zostało w jednostce przez firmę zewnętrzną 1 sprawdzenie audytowe w ramach dostawy licencji i wdrożenia oprogramowania, przeprowadzenia modernizacji systemów dziedzinowych, uruchomienia e-usług publicznych, digitalizacji i udostępniania zasobów informacji przestrzennej z dostawą oprogramowania i sprzętu informatycznego, o czym szczegółowo w punkcie 2.9.

[akta kontroli str. 372-385]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z nieprawidłowościami.

2.2. Analiza zagrożeń związanych z przetwarzaniem informacji

Z § 20 ust. 2 pkt 3 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy.*

Wymogiem skuteczności SZBI jest przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji. Kluczowa rola analizy ryzyka wynika z faktu, że rodzaj i poziom zastosowanych zabezpieczeń jest względny i jest zależny od ważności aktywów informatycznych danego podmiotu.

Zgodnie z wymogiem wynikającym z § 20 ust. 2 pkt 3 rozporządzenia KRI,), w 2018 roku przeprowadzana była w Urzędzie wstępna analiza ryzyka bezpieczeństwa informacji. W ramach przeprowadzonej analizy dokonano oszacowania ryzyka dla bezpieczeństwa danych oraz opracowano katalog (rejestr) zagrożeń/incydentów naruszenia przepisów o ochronie danych.

Zgodnie z zapisami przyjętej Polityki Bezpieczeństwa str. 10 - *w wyniku szacowania ryzyka powinien powstać dokument, który powinien być cyklicznie sporządzany, nie rzadziej niż raz w roku oraz przy każdej zmianie czynników powodujących zagrożenie*. Z dokumentacji przedstawionej kontrolującemu nie wynikało aby w 2019 roku analiza ryzyka została uaktualniona zgodnie z przyjętym obowiązkiem, co stanowi nieprawidłowość.

Z wyjaśnienia uzyskanego z Urzędu Gminy w powyższej sprawie wynika, że cyt.: *„Brak okresowej analizy i szacowania ryzyka wynikał z problemów komunikacyjnych z ASI (dowód: Protokoły z przeglądów). Administrator danych został poinformowany o problemach i braku*

możliwości realizacji tych zadań w połowie roku".

Mając powyższe na uwadze należy stwierdzić, że obowiązek wynikający z § 20 ust. 2 pkt 3 rozporządzenia KRI oraz przyjętej Polityki, w zakresie 2019 roku nie został spełniony (skutek – naruszenie powyższego przepisu). Osobami odpowiedzialnymi za powstanie nieprawidłowości są IOD oraz Kierownik kontrolowanej jednostki.

[akta kontroli str. 386-392, 405, 442]

Jednocześnie należy wskazać, iż zgodnie z art. 30 ust. 1 RODO, w jednostce jest opracowany i prowadzony rejestr czynności przetwarzania danych.

[akta kontroli str. 393-402]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z nieprawidłowościami.

2.3. Inwentaryzacja sprzętu i oprogramowania informatycznego

Z § 20 ust. 2 pkt 2 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: utrzymanie aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.*

W wyniku prowadzonych czynności, kontrolujący stwierdził brak aktualnej inwentaryzacji sprzętu komputerowego użytkowanego w Urzędzie Gminy Jedwabno, sporządzonej zgodnie z § 20 ust. 2 pkt 2 rozporządzenia KRI oraz zgodnie z załącznikiem nr 4 do przyjętej Polityki Bezpieczeństwa. Przedmiotowa inwentaryzacja zgodnie z cyt. powyżej przepisami powinna obejmować miedzy innymi rodzaj i konfigurację sprzętu.

Z wyjaśnienia uzyskanego z Urzędu Gminy w powyższej sprawie wynika, że cyt.: *„Nie przeprowadzono inwentaryzacji sprzętu i zasobów IT z winy pracownika".*

Zgodnie z przyjętym Programem kontroli nie sporządzanie bieżącej i aktualnej informacji nt. sprzętu i oprogramowania wykorzystywanego do przetwarzania informacji stanowi uchybienie, skutkujące naruszeniem z § 20 ust. 2 pkt 2 rozporządzenia KRI. Osobami odpowiedzialnymi za powstanie uchybienia są: ASI (Informatyk) oraz Kierownik kontrolowanej jednostki.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

[akta kontroli str. 217, 404, 443]

2.4. Zarządzanie uprawnieniami do pracy w systemach informatycznych

Stosownie do:

- § 20 ust. 2 pkt 4 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;*
- § 20 ust. 2 pkt 5 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie bezzwłocznej zmiany uprawnień, w przypadku zmiany zadań osób, o których mowa w pkt 4.*

Istotnym elementem polityki BI jest zarządzanie dostępem do systemów teleinformatycznych przetwarzających informacje. Zarządzanie dostępem ma zapewnić, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków, a w przypadku zmiany zadań następuje również zmiana ich uprawnień.

Zasady nadawania i odbierania uprawnień do przetwarzania danych osobowych oraz do pracy w systemie informatycznym określone zostały zarządzeniem Nr 80/2018 Wójta Gminy Jedwabno z dnia 27 lipca 2018 r. wprowadzającym Politykę Bezpieczeństwa w Urzędzie Gminy Jedwabno (zmiana - zarządzenie Nr 116/2018 Wójta Gminy Jedwabno z dnia 15 listopada 2018 r.).
Zasady nadawania i odbierania uprawnień do przetwarzania danych osobowych oraz zasady nadawania uprawnień do pracy w systemie informatycznym opisane są w zał. 2 (polityka bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych) oraz zał. 3 (polityka bezpieczeństwa danych osobowych przetwarzanych w systemach informatycznych) powoływanej powyżej polityki.

[akta kontroli str. 150-151, 158-163, 173-1841]

Osoby posiadające dostęp do danych osobowych posiadały pisemne upoważnienie. Prowadzona była też ewidencja osób upoważnionych do przetwarzania danych osobowych oraz elektroniczna ewidencja nadanych uprawnień w systemach. Pracownikom posługującym się systemem teleinformatycznym wydane zostały stosowne upoważnienia do pracy w określonym systemie.

W powyższym zakresie stwierdzono następujące nieprawidłowości:

- w prowadzonej ewidencji osób posiadających upoważnienie do przetwarzania danych osobowych, kontrolujący stwierdził brak wpisów, w przypadku wydania upoważnień dla 2 pracowników w 2019 r. oraz 1 w 2020 roku.

Z wyjaśnienia uzyskanego z Urzędu Gminy w powyższej sprawie wynika, że brak wpisów w ewidencji wynika z niedopatrzenia IOD. Skutkiem braku wpisów w ewidencji jest

utrudniona kontrola i nadzór jednostki nad wydanymi upoważnieniami. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD jednostki.

[akta kontroli str. 594-599, 606, 608, 612]

W powyższym zakresie stwierdzono następujące uchybienia:
- ewidencja osób posiadających upoważnienia do przetwarzania danych osobowych, prowadzona jest na innym druku niż wynika to z przyjętej w Urzędzie polityki bezpieczeństwa.
- upoważnienia do przetwarzania danych osobowych, wydawane są na innym druku niż wynika to z przyjętej w Urzędzie polityki bezpieczeństwa.

Z wyjaśnienia uzyskanego z Urzędu Gminy w powyższej sprawie wynika, że, cyt.: *„Wzór upoważnienia powstał w 2018 r. w sytuacji niedoprecyzowanej opinii UODO w tym zakresie. W miarę zmian prawa i pojawiających się wskazań był modyfikowany. Przygotowana, jeszcze nie przyjęta nowa wersja PB zawiera inną, bardziej adekwatną wersję z adnotacją o możliwości modyfikacji"*. Stosowanie odmiennych wzorów dokumentacji nie wpływa na realizację zadania, skutkuje jednakże rozbieżnościami w wytworzonej w danej sprawie dokumentacji. Osobą odpowiedzialną za powstanie uchybienia jest IOD jednostki.

[akta kontroli str. 231, 262, 443, 534, 600-615]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z nieprawidłowościami.

2.5. Szkolenia pracowników zaangażowanych w proces przetwarzania informacji

Z § 20 ust. 2 pkt 6 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich.*

Z dokumentacji przedstawionej kontrolującemu wynika, że pracownicy Urzędu Gminy Jedwabno zaangażowani w proces przetwarzania informacji, uczestniczyli łącznie w okresie objętym kontrolą w 21 szkoleniach (zorganizowanych przez IOD), dotyczących aspektów RODO, ochrony danych osobowych, bezpieczeństwa teleinformatycznego, tj.:
- w 2018 roku przeprowadzono 10 szkoleń, w tym 5 szkolenia - pojedyncze osoby, 5 szkoleń zbiorowych.
- w 2019 roku przeprowadzono 9 szkoleń, w tym 3 szkolenia - pojedyncze osoby, 6 szkoleń zbiorowych.
- w 2020 roku do dnia kontroli przeprowadzono 2 szkolenia (pojedyncze osoby).

[akta kontroli str. 318-347]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.6. Praca na odległość i mobilne przetwarzanie danych

Zgodnie z § 20 ust. 2 pkt 8 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: ustanowienie podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość.*

Procedura bezpieczeństwa komputerów przenośnych zawarta została w załączniku nr 12 do zarządzenia Nr 80/2018 Wójta Gminy Jedwabno z dnia 27 lipca 2018 r. wprowadzającego Politykę Bezpieczeństwa w Urzędzie Gminy Jedwabno.

[akta kontroli str. 206-207]

Z uzyskanych podczas kontroli informacji wynika, że sprzęt informatyczny w zakresie systemów teleinformatycznych wykorzystywany jest tylko w siedzibie jednostki.
Przedmiotowe cząstkowe zagadnienie ze względu na wykorzystywanie sprzętu w zakresie systemów teleinformatycznych tylko w siedzibie jednostki (stacjonarny tryb pracy) nie podlegało ocenie.

2.7. Serwis sprzętu informatycznego i oprogramowania

Stosownie do § 20 ust. 2 pkt 10 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zawieranie w umowach serwisowych podpisanych ze stronami trzecimi zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji.*

W przypadku systemów informatycznych niezbędne jest objęcie tych systemów (w zakresie oprogramowania użytkowego i systemowego, sprzętu oraz rozwiązań telekomunikacyjnych) stosownymi umowami serwisowymi, gwarantującymi odpowiednio szybkie uruchomienie pracy systemu w przypadku awarii oraz gwarantującymi bezpieczeństwo informacji (BI) dla informacji uzyskanych przez wykonawców w związku z ich realizacją.

[redacted]

[akta kontroli str. 406-419]

W ramach prowadzonych czynności kontrolnych stwierdzono, że Urząd Gminy zawarł z firmą [redacted] stosowną umowę powierzenia danych na

wypadek awarii systemu oraz konieczności ingerencji firmy jako autora oprogramowania w bazy danych zawierające dane osobowe.

[akta kontroli str. 420-441]

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.8. Procedury zgłaszania incydentów naruszenia BI

Z § 20 ust. 2 pkt 13 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: bezzwłoczne zgłaszanie incydentów naruszenia bezpieczeństwa informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących.*

Instrukcja postępowania w przypadku stwierdzenia zagrożenia w postaci naruszenia ochrony danych osobowych została uregulowana Zarządzeniem Nr 80/2018 Wójta Gminy Jedwabno z dnia 27 lipca 2018 r. wprowadzającym Politykę Bezpieczeństwa w Urzędzie Gminy Jedwabno. (zał. 15, 16, 21).

[akta kontroli str. 152-153, 250-260, 269-270]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.9. Audyt wewnętrzny z zakresu bezpieczeństwa informacji

Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.*

Na podstawie okazanej dokumentacji kontrolujący stwierdził, iż w okresie objętym kontrolą tj. od 1 stycznia 2018 r. do dnia rozpoczęcia czynności kontrolnych (26 lutego 2020 r.), przeprowadzone zostało w jednostce 1 zadanie audytowe:

- w 2018 roku – stwierdzono brak przeprowadzenia audytu wewnętrznego w zakresie bezpieczeństwa informacji. Powyższy brak ocenić należy jako nieprawidłowość.

  Z wyjaśnienia uzyskanego z Urzędu Gminy w powyższej sprawie wynika, że cyt.: *„W 2018 r. została przeprowadzona analiza ryzyka dla Urzędu Gminy w związku z wdrożeniem RODO. Przyjęliśmy, ze na etapie czekających nas istotnych zmian systemu (EDICTA) taka analiza jest wystarczająca".*

  Brak przeprowadzenia audytu wewnętrznego w zakresie bezpieczeństwa informacji skutkuje niedopełnieniem obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI. Osobą odpowiedzialną za powstanie nieprawidłowości jest IOD kontrolowanej jednostki.

- w 2019 roku przeprowadzone zostało przez firmę zewnętrzną 1 sprawdzenie audytowe

w ramach dostawy licencji i wdrożenia oprogramowania, przeprowadzenia modernizacji systemów dziedzinowych, uruchomienia e-usług publicznych, digitalizacji i udostępniania zasobów informacji przestrzennej z dostawą oprogramowania i sprzętu informatycznego.

- w przypadku roku 2020 r., istnieje jeszcze możliwość przeprowadzenia przez jednostkę audytu bezpieczeństwa informacji (do końca bieżącego roku). Wobec powyższego dopełnienie obowiązku wynikającego z § 20 ust. 2 pkt 14 rozporządzenia KRI, w zakresie roku 2020, nie podlegało ocenie.

[akta kontroli str. 372-385, 404, 443]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z nieprawidłowościami.

2.10. Kopie zapasowe

Z § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: minimalizowanie ryzyka utraty informacji w wyniku awarii.*

Jednym z kluczowych sposobów zapobiegania utracie informacji w wyniku awarii jest wykonywanie kopii zapasowych. Tworzenie kopi zapasowych jest elementem planu ciągłości działania. Celem tworzenia kopii zapasowych jest możliwość odzyskania danych i przywrócenia do pracy użytkowej systemu teleinformatycznego wraz z informacjami przechowywanymi przez ten system, np. w bazie danych. Wymóg ten można osiągnąć wykonując regularnie kopie zapasowe całego środowiska pracy danego systemu teleinformatycznego, tj. systemu operacyjnego, jego konfiguracji (w tym konfiguracji zabezpieczeń), systemu informatycznego i informacji w nim przechowywanych.

Zasady tworzenia kopii zapasowych uregulowane zostały Zarządzeniem Nr 80/2018 Wójta Gminy Jedwabno z dnia 27 lipca 2018 r. wprowadzającym Politykę Bezpieczeństwa w Urzędzie Gminy Jedwabno (zał. nr 7 *Procedura tworzenia kopii*).

[akta kontroli str. 194-195]

Zgodnie z wytycznymi zawartymi w przyjętej polityce kopie bezpieczeństwa wykonuje ASI. Zasady postępowania przy tworzeniu kopii zapasowych ujęte zostały w załączniku nr 7 do przyjętej polityki. Zgodnie z przyjętą dokumentacją SZBI, harmonogram tworzenia kopii zapasowych, dla poszczególnych zasobów informatycznych stanowi dokumentację wewnętrzną.

[redacted]

W przekazanej kontrolującemu dokumentacji nie stwierdzono opracowanego harmonogramu tworzenia kopii zapasowych, którego wymóg opracowania wynika wprost z przyjętej polityki. W powyższej sprawie kontrolujący otrzymał wyjaśnienia, cyt.: „[redacted]".

Brak opracowanego harmonogramu uniemożliwia weryfikację terminowości tworzonych kopii zapasowych, co stanowi uchybienie skutkujące naruszeniem § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI. Osobami odpowiedzialnymi za powstanie uchybienia są: ASI (Informatyk) oraz Kierownik kontrolowanej jednostki.

[akta kontroli str. 194-195, 404, 443, 489-533]

W przypadku wykonywania testów w celu sprawdzenia poprawności wykonywania kopii zapasowych oraz sprawdzenie przydatności utworzonych kopii podczas próby symulowanego przywrócenia i uruchomienia oprogramowania dziedzinowego po przywróceniu, zgodnie z zapisami przyjętej polityki, odpowiedzialność za okresowe sprawdzanie kopii pod kątem ich dalszej przydatności do odtworzenia w wypadku awarii systemu ponosi ASI. Ze względu na nieobecność ASI podczas kontroli, wykonanie tego zadania kontroler mógł zweryfikować na podstawie jedynego dostępnego dokumentu - „Lista zadań wykonywanych przez ASI w trybie tygodniowym", prowadzonego przez ASI w formie papierowej. Przedmiotowy dokument prowadzony był od 08.04.2019 r. do 30.08.2019 r. W tym okresie (zgodnie z zapisami w dokumencie) ASI dokonał weryfikacji wykonanych kopii zapasowych 11 razy.

Z otrzymanego z Urzędu Gminy wyjaśnienia wynika, że cyt.: „[redacted]".

[akta kontroli str. 443, 518-533]

Kontrolującemu nie przedstawiono żadnej dokumentacji potwierdzającej wykonywanie testów w celu sprawdzenia poprawności tworzonych kopii zapasowych w okresie od 01.01.2018 r. do 08.04.2019 r. oraz od 31.08.2019 r. do dnia kontroli.

Brak potwierdzenia w dokumentacji przedmiotowych czynności nie pozwala kontrolującemu jednoznacznie stwierdzić, że sprawdzenia poprawności tworzonych kopii zapasowych były faktycznie wykonywane. Powyższe należy zakwalifikować jako uchybienie skutkujące naruszeniem § 20 ust. 2 pkt 12 lit. b rozporządzenia KRI. Osobami odpowiedzialnymi za powstanie uchybienia są: ASI (Informatyk) oraz Kierownik kontrolowanej jednostki.

Należy wskazać, że regularne testowanie jakości kopii zapasowych jest kluczowym działaniem w celu minimalizowania ryzyka utraty informacji w wyniku awarii. Wskazane jest przechowywanie kopii zapasowych w innej lokalizacji niż miejsce ich tworzenia, w odległości niezbędnej do uniknięcia uszkodzeń spowodowanych przez katastrofę, która dotknęłaby podstawowy ośrodek przetwarzania danych.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

2.11. Projektowanie, wdrażanie i eksploatacja systemów teleinformatycznych

Stosownie do § 15 ust. 1 rozporządzenia KRI *systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.*

Wykorzystywane w Urzędzie systemy teleinformatyczne wspomagające realizację zadań z zakresu administracji rządowej dzieliły się na systemy centralne tj. ŹRÓDŁO i CEiDG oraz system wspierający zakupiony u dostawcy zewnętrznego - PUMA. Na obsługę aktualnie zainstalowanego oprogramowania z firmą dostarczającą system informatyczny zawarto stosowną umowę licencyjną (opieka autorska), gwarantujące rozwój systemu i dostosowanie do obowiązujących przepisów prawa. System teleinformatyczny, w razie awarii podlega ekspertyzie technicznej zlecanej firmie dostarczającej.

Mając powyższe na uwadze przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 406-419]

2.12. Zabezpieczenia techniczno-organizacyjne dostępu do informacji

Z § 20 ust. 2 rozporządzenia KRI wynika, że *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez:*

- pkt 7 *zapewnienie ochrony przetwarzania informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez: a) monitorowanie dostępu do informacji; b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji, c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;*
- pkt 9 *zabezpieczenie informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie;*
- pkt 11 *ustalenie zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych.*

W celu uzyskania odpowiedniego poziomu BI, przy jednoczesnym zapewnieniu właściwego do nich dostępu przez uprawnionych użytkowników stosowany jest szereg zabezpieczeń informatycznych. Celem zabezpieczeń jest uzyskanie ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, a także np. kradzieżą środków przetwarzania informacji.

Z wyjaśnień uzyskanych w Urzędzie Gminy wynika, że w celu zabezpieczenia danych będących w posiadaniu Urzędu oraz uzyskania maksymalnego poziomu bezpieczeństwa ich przetwarzania zastosowano, cyt.: „[redacted]".

[akta kontroli str. 444, 534-541]

Mając na uwadze powyższe wyjaśnienia przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

2.13. Zabezpieczenia techniczno-organizacyjne systemów informatycznych

Stosownie do:

- § 20 ust. 2 pkt 12 rozporządzenia KRI *zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez: zapewnienie odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na: a) dbałości o aktualizację oprogramowania; b) minimalizowaniu ryzyka utraty informacji w wyniku awarii; c) ochronie przed błędami, nieuprawnioną modyfikacją; d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa; e) zapewnieniu bezpieczeństwa plików systemowych; f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych; g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa; h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;*
- § 20 ust. 4 rozporządzenia KRI *niezależnie od zapewnienia działań, o których mowa w ust. 2, w przypadkach uzasadnionych analizą ryzyka w systemach teleinformatycznych podmiotów realizujących zadania publiczne należy ustanowić dodatkowe zabezpieczenia.*

W punkcie 2.12 wykazano mechanizmy jakie jednostka kontrolowana zastosowała w celu zapewnienia ochrony przetwarzanych informacji, w ramach badanych systemów teleinformatycznych przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami. Zapewniono również środki uniemożliwiające nieautoryzowany dostęp oraz zapewniające kontrolę dostępu do systemów teleinformatycznych służących do realizacji zadań zleconych z zakresu administracji rządowej, poprzez:

[redacted]

– [redacted].

Powyższe sprawdzono na wybranym stanowisku roboczym.

Podczas kontroli dokonano także oględzin pomieszczenia serwerowni Urzędu Gminy Jedwabno. W wyniku oględzin stwierdzono, że pomieszczenia budynku, w którym znajduje się serwerownia posiadają zabezpieczenie alarmowe. Urządzenia serwerowe umieszczono w specjalistycznej szafie. W pomieszczeniu zainstalowano urządzenie UPS chroniące przed spadkiem napięcia podawanego na urządzenia serwerowe. Pomieszczenie wyposażono w gaśnicę przystosowaną do gaszenia urządzeń pod napięciem. W pomieszczeniu zainstalowana jest czujka ruchu oraz czujka dymu. Pomieszczenie wyposażono w przenośny sprzęt monitorujący temperaturę i wilgotność. Okno pomieszczenia zabezpieczono stalową kratą.

[redacted].

Przyczyną powstania uchybień jest niedostosowanie pomieszczenia do pełnienia roli serwerowni, co skutkować może awarią urządzeń serwerowych i utratą danych. Osobą odpowiedzialną za powstanie uchybień jest kierownik kontrolowanej jednostki.

Powyższe potwierdza dokumentacja z przeprowadzonych oględzin.

[akta kontroli str. 616-622]

Przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie z uchybieniami.

2.14. Rozliczalność działań w systemach informatycznych

Stosownie do:

– § 21 ust. 2 rozporządzenia KRI *w dziennikach systemów odnotowuje się obligatoryjnie działania użytkowników lub obiektów systemowych polegające na dostępie do: 1) systemu z uprawnieniami administracyjnymi; 2) konfiguracji systemu, w tym konfiguracji*

zabezpieczeń; 3) przetwarzanych w systemach danych podlegających prawnej ochronie w zakresie wymaganym przepisami prawa;

- § 21 ust. 3 rozporządzenia KRI *poza informacjami wymienionymi w § 21 ust. 2 rozporządzenia KRI są odnotowywane działania użytkowników lub obiektów systemowych, a także inne zdarzenia związane z eksploatacją systemu w postaci: 1) działań użytkowników nieposiadających uprawnień administracyjnych, 2) zdarzeń systemowych nieposiadających krytycznego znaczenia dla funkcjonowania systemu, 3) zdarzeń i parametrów środowiska, w którym eksploatowany jest system teleinformatyczny – w zakresie wynikającym z analizy ryzyka;*
- § 21 ust. 4 rozporządzenia KRI *informacje w dziennikach systemów przechowywane są od dnia ich zapisu, przez okres wskazany w przepisach odrębnych, a w przypadku braku przepisów odrębnych przez dwa lata.*

Z wyjaśnień uzyskanych w Urzędzie Gminy wynika, że cyt.: *„Polityka zaleca przechowywanie logów 2 lata. W przypadku aplikacji PUMA, logi są przyrostowe i nie były ograniczane (brak zapisu w dzienniku o ograniczeniu logów)."*
Mając na uwadze powyższe przedmiotowe cząstkowe zagadnienie ocenia się pozytywnie.

[akta kontroli str. 444]

III. Zapewnienie dostępności informacji zawartych na stronach internetowych urzędów dla osób niepełnosprawnych

Uwzględniając potrzeby osób niepełnosprawnych podmiot publiczny powinien zastosować w eksploatowanych systemach teleinformatycznych rozwiązania techniczne umożliwiające osobom niedosłyszącym, niedowidzącym lub niewidomym zapoznanie się z treścią informacji, m.in. poprzez powiększenie czcionki, obrazu, zmianę kontrastu. Zgodnie z § 19 rozporządzenia KRI, w systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia KRI.

Systemy informatyczne wspomagające realizację zadań zleconych z zakresu administracji rządowej w Urzędzie, ze względu na brak interakcji z klientami zewnętrznymi za pośrednictwem publicznej sieci Internet nie są objęte wymogami WCAG 2.0.
Strona internetowa BIP Urzędu Gminy zawiera elementy umożliwiające zmianę wielkości czcionki w celu ułatwienia korzystania z treści na niej zawartych przez osoby niedowidzące. Zmiany wielkości czcionki dokonuje się przy pomocy ikony – A + (umieszczonej w prawym górnym rogu). Zgodnie z załącznikiem nr 4 do rozporządzenia KRI, strona BIP spełniała poniższe zasady:

- postrzeganie – informacje oraz komponenty interfejsu strony były przedstawione użytkownikom w sposób dostępny dla jego zmysłów,

- funkcjonalność – komponenty interfejsu stron umożliwiały korzystanie z nich,
- zrozumiałość – informacje oraz obsługa interfejsu były zrozumiałe.

W przypadku strony www. Urzędu, brak jest zamieszczonych na niej narzędzi umożliwiających zmianę wielkości czcionki lub zmianę kontrastu strony, w celu ułatwienia korzystania z treści na niej zawartych przez osoby niedowidzące. Strona nie spełnia zasady zawartej w załączniku nr 4 do rozporządzenia KRI, - postrzeganie - która to zasada stanowi, że informacje oraz komponenty interfejsu strony powinny być przedstawione użytkownikom w sposób dostępny dla jego zmysłów. Powyższe stanowi nieprawidłowość. Osobą odpowiedzialną za powstanie nieprawidłowości jest ASI (Informatyk).

Każda strona dostępna w Internecie powinna zapewniać maksymalne wsparcie wszystkim grupom wiekowym jak i społecznym. Warunkiem dostępności strony jest dobry kontrast zapewniający swobodny odczyt przedstawionych informacji. Im wyższy jest kontrast, tym łatwiej odróżnić obiekt, zdjęcie czy tekst pierwszego planu od tła. Niski poziom kontrastu utrudnia korzystanie z witryny przede wszystkim użytkownikom o mniejszej ostrości wzroku, a także osobom niedowidzącym. Celem ułatwienia postrzegania tekstu użytkownikom niedowidzącym można również umożliwić zmianę wielkości tekstu bez utraty jego czytelności lub funkcjonalności serwisu internetowego. W tym celu można wprowadzić udogodnienia w postaci ikonek typu „**aAA**", które po kliknięciu nadadzą stronie odpowiedni rozmiar.

Walidacja za pomocą narzędzia http://wave.webaim.org tj. walidatora WAVE-WCAG 2.0 dla strony BIP wykazała 2 błędy, dla strony www. Urzędu 16 błędów.

[akta kontroli str. 299, 302, 623, 624]

Powyższe zagadnienie oceniono pozytywnie z nieprawidłowościami.

Do ustaleń kontroli nie zostały wniesione zastrzeżenia.

IV. Zalecenia

Mając na uwadze powyższe ustalenia i oceny wnoszę o:

1. Przeprowadzanie sprawdzeń/przeglądów infrastruktury IT Urzędu Gminy oraz stanowisk roboczych zgodnie z przyjętym harmonogramem, w celu doskonalenia systemu zarządzania bezpieczeństwem informacji i utrzymywania go na odpowiednio wysokim poziomie.
2. Zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI oraz zapisami przyjętej w Urzędzie Polityki Bezpieczeństwa, przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko.

3. Zgodnie z § 20 ust. 2 pkt 3 rozporządzenia KRI oraz zgodnie z załącznikiem nr 4 do przyjętej Polityki Bezpieczeństwa, sporządzanie bieżącej i aktualnej informacji nt. sprzętu IT i oprogramowania wykorzystywanego do przetwarzania informacji.
4. Prowadzenie ewidencji osób posiadających upoważnienia do przetwarzania danych osobowych w sposób rzetelny i pełny. Wydawanie przedmiotowych upoważnień na obowiązujących drukach, zgodnych z przyjętą Polityką Bezpieczeństwa.
5. Zapewnienie w jednostce nie rzadziej niż raz na rok okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, zgodnie z § 20 ust. 2 pkt 14 rozporządzenia KRI.
6. Opracowanie harmonogramu oraz regularne testowanie jakości wytworzonych kopii zapasowych poprzez odtworzenie danych systemu informatycznego z wytworzonej kopii. Każdorazowe dokumentowanie wykonywanych testów poprawności tworzonych kopii zapasowych.
7. W miarę możliwości finansowych Urzędu wydzielenie serwerowni jako osobnego pomieszczenia przeznaczonego wyłącznie pod potrzeby infrastruktury serwerowej. Zabezpieczenie pomieszczenia serwerowni poprzez montaż: wzmocnionych drzwi wejściowych o podwyższonej odporności ogniowej, urządzenia klimatyzującego, ponadto wyposażenie serwerowni w stacjonarny sprzęt monitorujący temperaturę i wilgotność.
8. Dostosowanie strony www. Urzędu, do wymagań Web Content Accessibility Guidelines (WCAG 2.0), z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia KRI.

Proszę Pana Wójta o podjęcie działań mających na celu usunięcie stwierdzonych nieprawidłowości i uchybień oraz o poinformowanie Wojewody Warmińsko – Mazurskiego w terminie 14 dni od dnia otrzymania niniejszego wystąpienia, o sposobie wykorzystania uwag i wniosków oraz wykonania zaleceń, a także o podjętych działaniach lub przyczynach niepodjęcia działań.

Jednocześnie informuję, że stosownie do art. 48 ustawy o kontroli w administracji rządowej od wystąpienia pokontrolnego nie przysługują środki odwoławcze.

WOJEWODA
WARMIŃSKO-MAZURSKI

Artur Chojecki

Potwierdzam zgodność kopii wydruku z dokumentem elektronicznym:

Identyfikator dokumentu	1931884.4467102.3849627
Nazwa dokumentu	WP systemy teleinformatyczne UG JEDWABNO.pdf
Tytuł dokumentu	WP systemy teleinformatyczne UG JEDWABNO
Sygnatura dokumentu	FK-IV.431.5.2020
Data dokumentu	2020-04-02
Skrót dokumentu	C2B9059189F06F2A731906EC7F4DCFEE54D855DD
Wersja dokumentu	1.5
Data podpisu	2020-04-02 13:54:46
Podpisane przez	Artur Henryk Chojecki WOJEWODA

EZD 3.96 1.1.31187

Data wydruku: 2020-06-26
Autor wydruku: GAZDA RADOSŁAW (inspektor wojewódzki)